STATE OF ALABAMA

Information Technology Procedure

PROCEDURE 603P1-01: SECURITY COUNCIL

To enhance the level of information security, protect State information and data against internal and external threats, and to ensure compliance with State information security policies, procedures, and standards the Information Services Division (ISD) Director has established the State Information Technology (IT) Security Council. This document identifies Security Council membership and procedures. The target audience for these procedures is the State of Alabama employees, contractors, vendors, or business partners who participate in the State IT Security Council process.

OBJECTIVE:

Implement the requirements of State IT Policy 603: Security Council.

SCOPE:

These procedures apply to the State of Alabama employees, contractors, vendors, and business partners who participate in the State IT Security Council process.

SECURITY COUNCIL MEMBERSHIP

Security Council membership shall include individuals serving in the following positions:

Voting Members:

All ISD Assistant Directors shall serve as voting members of the council.

Any voting member unable to attend a council meeting should send an alternate to the meeting to vote on their behalf. No voting member may cast more than one vote. In the event of a tie vote or if the matter cannot be resolved by the council it will be escalated to the ISD Director for a decision.

Advisory (non-voting) Members:

- ISD Chief Information Security Officer (CISO) - Council Leader
- ISD Network Operations Manager
- ISD Mainframe Systems Manager
- ISD Systems Administration Manager
- ISD Security Business Partner(s) representatives
- Other personnel when requested to attend
- At-large members (4)

At-large members shall be selected IT Managers, Information Security Officers, or security administrators from agencies other than the Department of Finance/ISD. Four at-large members shall be selected annually by the voting members of the council, and will participate in all council proceedings for 12 consecutive months. At-large members do not vote but are encouraged to send an alternate to the meetings if they cannot attend.

COUNCIL SCHEDULE

Meetings:

The Security Council will meet quarterly (normally on the second Wednesday of the second month in each quarter: February, May, August, and November) for routine business and for emergency sessions at the call of the Council Leader. Two meetings shall be required annually; additional meetings will be scheduled as needed.

Pre-meeting Conference Call:

If necessary, a pre-meeting conference call will be conducted one week prior to the meeting date. The call may be necessary to discuss complex topics or to verify that the appropriate personnel have reviewed and are ready to discuss agenda items.

SECURITY EVALUATION PROCESS

The following illustrates the 4-phased process the Security Council will use to identify issues, gather key information, present data to Council members for review and recommendation, and follow up on the implementation to ensure that approved changes are properly made and the required level of security is present to protect State information systems and data.

Initiation:

Changes to the baseline configuration of the State infrastructure can be initiated by various events or by any entity including customers, application developers, staff, vendor upgrades, or changes to external requirements. Requests for changes or recommendations may be brought to the Security Council by a customer with a known security issue, or a customer may have an IT issue with security implications such as making an application accessible via the Internet. A security-related incident, or other incident that reveals evidence of a security issue, may also require Security Council action. Regardless of how the issue comes to be identified as a security matter, the ISD Help Desk must be informed so a Work Order can be initiated (by anyone), assigned to the Security group, and tracked.

Table 1: Initiation

Initiation Phase	
Input:	Issue/request information
Activities:	I1. Security Council Leader (LDR) or other security group personnel receive request and open Work Order with Help Desk or receive Work Order from Help Desk. I2. LDR assigns Work Order to Analyst(s); copies Security Council Recorder (RCDR) I3. RCDR adds item to council agenda.
Output:	Work Order and any additional issue/request information Council agenda

Analysis:

Assigned personnel analyze the issue/request, address all security concerns, and prepare a summary of findings and recommendations to present at a designated future council meeting.

Table 2: Analysis

Analysis Phase	
Input:	Work Order and any additional issue/request information
Activities:	The assigned analyst(s) shall: A1. Review issue /request. A2. Collect any additional information necessary. A3. Analyze and develop recommendations. A4. Document summary and recommendations. A5. Submit all artifacts to RCDR or LDR.
Output:	Completed summary and recommendations and other artifacts

Review:

The Security Council reviews the analysis summary and makes the determination whether or not to proceed with the change. If the Security Council determines that the plan/request should be disapproved, feedback is provided to the submitter. If the Security Council does not feel that the change is within their scope, the request will be escalated as required.

Table 3: Review

Review Phase	
Input:	Completed summary, recommendations, and other artifacts Council agenda
Activities:	R1. LDR or RCDR distributes or posts agenda and artifacts for council member review. R2. Council members review artifacts; prepare for discussion and/or decision. R3. LDR initiates meeting request for conference call. R4. Briefly discuss issue on conference call. Determine if sufficient info is available to make decision. If so bring to vote, else task for further analysis or defer until meeting for further discussion. R5. RCDR removes from agenda any action items closed during conference call; provides final agenda to LDR. R6. LDR initiates meeting request for monthly council meeting; sends agenda to invitees. R7. Council meets to discuss agenda items and open action items. If no decision is reached, unresolved matters shall be escalated as appropriate.
Output:	Council decision or recommendation Council agenda

Closure:

To make the final determination that the implemented change meets all requirements for the security of the State networks and safeguard of data, the Security Council may direct or recommend a risk assessment or independent verification and validation be conducted after implementation.

Table 4: Closure

Closure Phase	
Input:	Council decision/recommendation
Activities:	C1. LDR notifies initiator/requester of decision or recommendation C2. Implementation actions (may include verification of implementation as directed or recommended, risk assessment, policy changes, etc.), as directed by the Council. C3. RCDR documents decision in meeting minutes. C4. RCDR archives all artifacts. C5. LDR documents decision/actions in Work Order and closes Work Order when issue is resolved.
Output:	Archived artifacts Closed Work Order

Right to Appeal:

Agency Heads or IT Managers have the right to appeal if they disagree with the Security Council's decision. All appeals shall be made to the Director, Information Services Division.

ADDITIONAL INFORMATION:

Information Technology Policy 603: Security Council
http://cybersecurity.alabama.gov/documents/Policy_603_Security_Council.pdf

Information Technology Guideline 600-05G1: Configuration Management Process
http://cybersecurity.alabama.gov/documents/Guideline_605G1_CM_Process.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
600-03P1	1/12/2007	Original
600-03P1_A	2/6/2007	Added new voting member, AD Operations, and tie-break procedures.
600-03P1_B	3/22/2007	Changed at-large membership from 3 months to 1 year.
600-03P1_C	10/19/2007	Added new voting member, AD Applications Integration; increased at-large members to four.
600-03P1_D	1/15/2008	Updated voting member positions per policy change.
600-03P1_E	3/26/2008	Modified security evaluation request process to eliminate SER form.
603P1-00	5/10/2011	New number and format.
603P1-01	10/19/2011	Modified meeting schedule and conference call requirements